BT Yönetiminde Bilgi Sızıntısı ve Ağ Tabanlı Çoklu Protokol Bilgi Sızıntısı Engelleme

Burak Oğuz[1] H. Kerem Cevahir[2]

[1,2]Medra Teknoloji, Ankara

[1]e-posta: burak.oguz@gmail.com [2] e-posta: hkerem@gmail.com

Özetçe

Kurum ve kuruluşlar için bilgi sızıntısı rekabet ve itibar açılarından her geçen gün artan bir risk oluşturmaya başlamıştır. Bilgi güvenliğinin sağlanmasında önemli bir yere sahip olan sızıntının saptanması, kayıt altına alınması ve engellenmesi konusu yönetimsel olarak birçok standart ve en iyi uygulamada yerini almaya başlamış ve bu konuda birçok uygulama ortaya çıkmıştır. Bu makalede, ilk önce bilginin kurumsal yapısı ve bilgi sızıntısı ile ilgili bilgiler verilmiştir. Daha sonra COBIT ve ISO/IEC 27002 gibi standartlar ve en iyi uygulamalar açısından bilgi sızıntısının engellenmesi için gerekli denetimler incelenmiştir. Son olarak, bu standart ve en iyi uygulamaları iş gereksinimleri bakımından karşılayabilecek bilgi sızıntısı uygulaması ile ilgili genel bilgi verilmiştir.

1. Giriş

Klasik güvenlik anlayışının aksine, bilgi merkezli güvenliğin sağlanması için bilginin bilişim sistemleri üzerinden dışarıya akışını kontrol etmek gereklidir. Bilgi sızıntısı saptamak ve engellemek, uygulama seviyesi güvenlik duvarı, derinlemesine veri inceleme, güvenilir kayıt tutma konularını farklı yaklaşımlarla birleştirerek bir ağdaki bilgi akışını takip etmeyi ve istenilen profillere zorlamayı sağlamakla gerçekleştirilebilir.

Dışarıya veri akışının mümkün olduğu her ağda, veri sızıntısı riski bulunmaktadır. Kritik verilerin saklandığı ya da kullanıldığı ağlarda bu riskin önemi daha da artmaktadır. Geleneksel güvenlik duvarı yaklaşımları ve çok kullanılan iletişim protokollerinin yetersiz, dolayısıyla güvensiz olması da bu riskin boyutunu arttırmaktadır. Bugün uygulama seviyesinde inceleme yapan saldırı tespit sistemleri gibi ürünler, dışarıdan gelen tehditlere odaklanmaktadır ve riski sadece saldırı kapsamına daraltmaktadır. Dolayısıyla bu ve benzeri yaklaşımlar içeriden dışarıya veri sızıntısı riskini yok edememektedirler. Bu noktada devreye giren ağ tabanlı bilgi sızıntısı saptama ve engelleme sistemleri ile popüler iletişim protokollerindeki veri aktarım girişimleri incelenebilir, akan bilgi sınıflandırılabilir, inceleme sonuçlarına göre girişim güvenilir (kanıt olarak kullanılabilecek) bir şekilde kayıt altına alınabilir ya da engellenebilir.

Günümüzde BASEL II, GLBA, Sarbanes-Oxley, HIPAA ve DSS gibi akreditasyonlar ve standartlar, iletişim protokollerinden yapılan veri akışlarını izlemeyi ve kontrol altına almayı zorunlu hale getirmektedirler. Posta arşivi gibi ürün başlıkları da bu amaca hizmet etmektedir. Bilgi sızıntısının saptanması ve engellemesi bu yaklaşımı yatay ve dikey genişletmeyi hedeflemektedir. Hem daha fazla iletişim protokolünü destekleyip kayıt altına almayı, hem de engelleme ve derinlemesine veri inceleme gibi özelliklerle kontrolün kapsamını arttırmayı amaçlamaktadır.

Bu tarz akreditasyon ihtiyaçlarının zamanla daha çok uygulanmaya başlanması ile aslında yapılmak istenen büyük kurum ve kuruluşların birlikte işlerlik ve gerek maliyet ve gerekse de performans gereksinimlerinden dolayı bilginin daha açık ve ulaşılabilir hale getirilmesi, veri sızıntısının takibini klasik güvenlik anlayışının dışına taşmasına sebep olmuştur. Akreditasyonların gerçekleştirilmesi için kullanılan COBIT[1] ve ISO/IEC 27002[2] gibi en iyi uygulamalarında zaten bu tarz güvenlik ihtiyaçlarını risk başlıkları altında toplamışlardır.

İş açısından bilgi sızıntısı sistemleri incelendiği zaman ise mutlaka yatırımın geri dönüşünün yüksek olması beklenmektedir. Bu yüzden yatırımın geri dönüşünün sağlanması, operasyonların geliştirilmesi ve rekabet açısından bir bilgi sızıntısı ürünü şu özelliklere sahip olması gerekmektedir.

- Risk yönetimi
- Yasal düzenlemelere uyumluluk
- Operasyonel verimlilik
- Rekabetin korunması

2. Bilgi Sızıntısı

Bilgi sızıntısı riskinin öneminin anlaşılması için ilk önce kurum ve kuruluşların her gün üzerinde çalıştıkları verinin türünün ve öneminin belirlenmesi gerekmektedir. Bilgi, kurumlar için ulusal güvenliği ilgilendiren bilgilerden, kimlik bilgilerine kadar uzanan geniş bir yelpazede yer alırken kuruluşlar açısından rekabetin ve operasyonel faaliyetlerin devamlılığının sağlanması için gerekli fikri mülkiyetlerden, kuruluş içi gizli bilgilere kadar genişletilebilir. Kuruluşlar için bilgi tiplerinin detayları Tablo 1'de verilmiştir.

Tablo 1: Kuruluş bilgi tipleri ve örnekleri

Bilgi Tipi	**Örnek**
Müşteri bilgisi	Kişisel sağlık bilgilerinin gizliliği Kişisel finansal bilgilerin gizliliği Müşteri bilgileri Sipariş geçmişi
Fikri haklar	Ürün tanımları ve tasarım detayları Pazar araştırmaları
Gizli bilgiler	Satış planları Dağıtım planları Finansal planlar

Genel olarak baktıldığında bilgi sızıntısı riski, sızması sonucunda yasal, maddi veya ulusal güvenlik konularında sonuçları olabilecek bilginin korunması tercihinin yapılması olarak özetlenebilir.

2.1. Bilgi sızıntısı kaynakları

Bilgi sızıntısı kaynakları itibariyle birçok nedeni bulunmaktadır. Yapılan araştırmaya göre[3] bilgi sızıntısının %80'lik kısmı çalışanların bilgi güvenliği politikalarını bilmemesinden kaynaklanmaktadır. Aynı araştırmaya göre, İngiltere'de bulunan kuruluşların %66'sı e-posta yoluyla yapılan iletişimde çalışan tarafından fikri hakların ve gizli bilgilerin bilinçli veya bilinçsiz olarak sızdırıldığını ve kuruluş çalışanları tarafından dışarıya gönderilen tüm e-postaların %12'lik kısmının yasal sorunlara yol açabileceği saptanmıştır. Doğal olarak bilgi sızıntısının oluşmasında bilgi sistemleri en üst sıralarda yer almaktadır. Yapılan araştırmalara göre bilgi sızıntısı bilgi sistemleri üzerinde %77,25 oranında ağ uygulamaları üzerinden gerçekleşmektedir [1] . Tablo 2'de kaynakları detaylı olarak görebiliriz.

Tablo 2: Bilişim sistemleri ortamları üzerinden bilgi sızıntısı oranları

Oran (%)	Kaynak
42,57	HTTP
15,84	E-Posta
10,89	Ağ yazıcısı
9,90	Güvenlik uygulamaları
6,83	USB aygıtlar
4,95	İç ağ e-posta
2,97	Web mail
0,99	Anında mesajlaşma protokolleri
5,03	Diğer

Araştırmalarda görüldüğü üzere bilgi sızıntısı yapısı itibariyle bilişim sistemleri üzerinden birçok ortam ve protokol üzerinden gerçekleşebilmektedir. En yüksek oranda özellikle HTTP protokolü üzerinden gerçekleşen bilgi sızıntısının kaynağı, çalışanların İnternet ve İnternet e-posta istemcilerini kullanmalarındaki eğitimsizlik ve bilinçsizlik olarak gösterilebilir.

2.2. Bilgi sızıntısının sonuçları

Bilgi sızıntısının sonuçları kurum ve kuruluşlar açısından ulusal ve iş boyutunda birçok önemli zarara neden olabilir. Yapılan araştırmalar [2] göstermektedir ki herhangi bir bilgi sızıntısı olayının ortalama maliyeti gerçekleştiği kuruma veya kuruluşa 1,82 milyon $ olarak hesaplanmıştır. Aynı araştırmanın devamında, bu araştırmaya katılan kuruluşların %77'lik kısmının bilgi sızıntısını tespit edebilecek durumda olmadığı dolayısıyla çıkartılan bu maliyete dâhil edilmedikleri belirtilmiştir.

Bilgi sızıntısının maddi sonuçları dışındaki, diğer olumsuz etkileri yasal kayıplar ve itibar kayıpları olarak belirtilebilir. Bütün sonuçlar, iş açısından incelendiği zaman iş ortaklıklarının bozulması, müşteri kaybetme ya da muhtemel müşteriler arasında rekabetin olumsuz etkilenmesi, ortaya çıkacak yasal işlemlerden doğacak olan ağır tazminatlar ve hak mahrumiyetleri olarak özetlenebilir.

[1] Ekim 2009 tarihi itibariyle erişilebilir durumdadır. http://www.surveilstar.com/prevent-data-leakage.html

[2] Ekim 2009 tarihi itibariyle erişilebilir durumdadır. http://www.eweek.com/c/a/Security/New-Report-Chronicles-the-Cost-of-Data-Leaks/

2.3. Bilgi sızıntısının BT yönetimi olarak incelenmesi

Bilgi güvenliği kavramı artık bir sonuç olmaktansa bilgi teknolojilerinin yönetimi sırasında riskleri en aza indirmek için bir yöntem olarak ele alınmaya başlanmıştır. Bilgi sızıntısının BT yönetimi içerisinde de önemli bir yeri bulunmaktadır. Bilgi sızıntısının, yönetim olarak ele alınabilmesi için ilk önce gerekli nitelikli bilginin belirlenmesi ve sınıflandırılması gereklidir.

Bilgi sızıntısı, 7 temel yönetim ölçütü açısından incelenirse şu 3 temel ölçütte iş açısından ilk öncelikli olduğu görülebilir.

1. Gizlilik: BT yönetiminde bilgi sızıntısına karşı gerçekleştirilecek kontroller, nitelikli bilginin gizliliğini sağlayacaktır. Bilginin gizli kalması gereken noktalarda bilgi sızıntısı olmadığının yönetimsel olarak belirlenmesi ve güvence altına alınması gerekmektedir.
2. Bütünlük: Üzerinde çalışılan değerli bilginin dışarıya sızması halinde iş gizliliği bozulacağı için işin bütünlüğü de etkilenmiş ve sağlanamamış olur. Bununla birlikte bilgi sızıntısının engellenmesinde kullanılacak uygulamanın kendi bütünlüğünü koruyabilmesi için güvenilir bilişim[4] gibi teknik gelişmelerden faydalanması gerekmektedir.
3. Devamlılık: Sızan bilginin niteliğine göre bilgi sistemlerinin devamlılığı da risk kapsamına girmiş olur. Ayrıca bilgi sızıntısının engellenmesinde kullanılacak uygulamanın devamlılığı da sanallaştırma[5] ile garanti altına alınmalıdır.

Bunların etkisiyle dolaylı olarak şu ölçütlerde ikincil olarak etkilenirler.

1. Yasal uyumluluk: Bilgi sızıntısının gerçekleşmesi ve işin yapılmasıyla ilgili güvenlik gereksinimlerinin karşılanılamaması sonucunda, yasal ve diğer iş uyumlulukları ile ilgili eksiklikler adli ve idari tazminatlara ve cezalara yol açabilir.
2. Güvenilirlilik: Bilgi sızıntısının oluşması ile ortaya çıkacak güvenlik zafiyeti tahsis edilmiş olan iş ortaklığı ve müşteri ilişkilerini olumsuz etkileyecek ve maddi kayıplara yol açacaktır.

Bilgi sızıntısına karşı yatırım yapılmadan önce mutlaka belirtilen ölçütler içerisinde risk hesaplaması yapılmalı ve yatırım geri dönüşü gerçekleşecek ise bu konuda yatırım yapılmalıdır. Kurum ve kuruluşlar için riskin hesaplanması için çeşitli yöntemler bulunmaktadır[6].

Bilgi sızıntısının saptanması ve değerlendirilebilir hale getirilmesi bu tarz sorunların, BT yönetimi içerisinde kar-zarar hesaplarının yapılabilmesini önemli kılmaktadır.

2.4. COBIT 4.1 çatısında bilgi sızıntısı

COBIT, bilgi teknoloji yönetimi için ISACA[7] ve ITGI[8] tarafından oluşturulmuş bir en iyi uygulamalar kontrol kümesidir. COBIT, yöneticilere, denetçi ve kullanıcılara genel kabul görmüş işlemler, işaretler ve en iyi uygulamalar sunarak, bilgi sistemlerinin bir kuruluş içerisindeki kullanımından en yüksek verimin ve kazancın, belirli yönetim ve denetimler içerisinde gerçekleştirilmesini sağlar[9]. COBIT'te tanımlanmış 4 kaynak, 34 süreç ve 215 denetim ölçütü bulunmaktadır. Başarı ölçütlerini, COBIT'te tanımlanan BT kaynakları ile birleştirilerek, bilgi sızıntısında hangi tür kaynakların tehlike altına girdiği Tablo 3'te gösterilmiştir.

Tablo 3: Bilgi sızıntısının yönetim ölçütleri ile BT kaynakları ilişkisi

	Uygulama	İnsan	Bilgi	Altyapı
Gizlilik			X	
Bütünlük	X		X	
Devamlılık	X		X	

COBIT'in 4 temel işlem grubu bulunmaktadır. Bu gruplar içerisinde bulunan işlemler ise kontrollerden oluşur. Bilgi sızıntısını bir risk olarak inceleyecek olursak, şu işlemlerin doğrudan uygulanmasında etkin olduğu görülebilir.

2.4.1. PO.02 – Bilgi mimarisinin tanımlanması

Planlama ve organizasyon grubu içerisinde bulunan bu işlemde, bütünlük birincil, gizlilik ise ikincil öncelikli ölçütler olarak belirlenmiştir. Bilgi mimarisi, güvenilir ve tutarlı bilgiye erişim ve uygulamaların iş sürecine uyumluluğunun sağlanması için bilginin bütünlüğü ve tutarlılığının bilginin sınıflandırılması şeklinde gerçekleştirilmesi ile elde edilir. Bilginin tasnifi, sızıntının engellenebilmesi için öncelikli bir süreç olarak belirlenmelidir. Bunun için şu aşamalar takip edilmelidir.

- İşte yetki sahibi herkesin planlama sürecine dâhil edilmesi,
- Veritabanında yapısal olarak veya dosyalarda yapısal olmadan bulunan hassas bilginin tanımlanması

2.4.2. PO.09 – BT risklerinin değerlendirilmesi ve yönetilmesi

Planlama ve organizasyon grubu içerisinde bulunan bu işlemde, gizlilik, bütünlülük ve devamlılık birincil öncelikli ölçütler olarak belirlenmiştir. BT risklerinin analiz edilmesi ve bu risklerin iş süreçleri ve amaçları üzerindeki etkisinin belirlenmesi gerekliliğinin sağlanması için gerçekleştirilen bir süreçtir. Bilgi sızıntısının ortaya çıkardığı riskler bu işlem içerisinde değerlendirilip, tesis edilecek bilgi sızıntısı saptama ve engelleme uygulamasının yeterlilikleri ve yetkinlikleri belirlenmelidir. Yetkinlik belirlenirken[11],

- İşte yetki sahibi herkesin planlama sürecine dâhil edilmesi
- Muhtemel veri sızıntısı yollarının teşhis edilmesi,
- Şu anki veri koruma yöntemlerinin hassas veri üzerindeki uygulamalarının gözden geçirilmesi,
- Kuruluşun tanımlı bir risk değerlendirmesi yaparak, mevcut veri koruma etkinliklerini değerlendirmesi,
- Risk değerlendirmesinin analiz edilmesiyle, kim, ne, nerede ve nasıl gibi soruların anlaşılması,
- Mevcut politikaların, risk değerlendirmesindeki sonuçlara göre değiştirilmesi,
- Yürürlüğe koyulacak eylemler ve iş akışı süreçlerinin belirlenmesi,
- Alınacak uygulama gereksinimlerinin belirlenmesi,
- Alınacak uygulamalar arasında değerlendirme yapılması,

aşamaları yürütülmelidir.

2.4.3. DS.05 – Sistem güvenliğinin sağlanması

Teslimat ve destek grubunda bulunan bu işlem içerisinde gizlilik ve bütünlük birincil, devamlılık ise ikincil ölçüt olarak belirlenmiştir. Sistem güvenliği sağlanırken, bilginin bütünlüğünün sağlanması ve güvenlik zayıflıklarının ve olaylarının etkilerinin en aza indirilmesi gerçekleştirilmesi zorunlu gereksinimlerdir. Bu süreç içerisinde kontroller gerçekleştirilirken, bilgi sızıntısının tespit engellenmesinde şu aşamalar dikkate alınmalıdır.

- Bilgi sızıntısı ile ilgili güvenlik planının, kuruluş kültürü de göz önünde bulundurularak yapılması ve gerekli bilgi sızıntısının engellenmesi için gerekli hizmet, personel, yazılım ve donanıma yatırım yapılması
- Kullanıcıların istenilen erişim seviyelerine hesap yönetiminin gerçekleştirilmesi ve gruplandırılması
- Kullanıcı gruplarının bilgi sızıntısı risklerine göre takip edilmesi ve gözetlenmesi
- Grupların bu eğilimlerine göre bilgi sızıntısı engelleme sistemi tarafından işlem kümelerine dâhil edilmesi
- Kullanıcı işlemlerinin kayıt altına alınması
- Ağ güvenliğinin sağlanması
- Hassas veri değişiminin düzenli ve denetlenmiş şekilde gerçekleştirilmesi

2.4.4. İzleme ve değerlendirme

COBIT ile BT yönetiminin tamamlanması için gerekli diğer bir işlem grubu da izleme ve değerlendirme işlemleridir. Bu işlemler içerisinde, bilgi sızıntısı saptama ve engelleme sonucu ortaya çıkan kayıtların performans, iç denetim ve BT sistemlerinin yönetimi süreçlerinde değerlendirilerek ortaya çıkan sonuçların, bilgi sızıntı riski, hassas veri, kullanılan protokoller ve sızıntı oluşturabilecek durumların tekrar gözden geçirilmesini sağlayacak yapıya getirilmesi gerekmektedir. Bu sayede, devamlı bir döngü içerisinde bilgi sızıntısı güvenlik politikaları güncellenmelidir.

2.5. ISO/IEC 27002 standardında bilgi sızıntısı

ISO/IEC 27002, gizlilik, bütünlük ve devamlılık boyutlarını da kapsayan, bilgi güvenliğinin sağlanması amacıyla iyi yapılandırılmış bir kontrol kümesi sunar. ISO/IEC 27002'yi, bilgi güvenliğinin sağlanması için amaç olmaktan öte, bilgi güvenliğinin sağlanması için gerekli bir el kitabı ya da menü olduğunu varsaymak daha doğru olacaktır.
ISO/IEC 27002 başlıkları, bilgi sızıntısının yol açabileceği bilgi güvenliği sorunları doğrultusunda incelenecek olursa şu başlıkların ilk öncelikli olarak ilintili olduğu görülebilir.

- Güvenlik politikasının oluşturulması aşamasında bilgi sızıntısının yol açabileceği bilgi güvenliği zayıflıklarının iş gereksinimleri ve yasal düzenlemeler çerçevesinden ele alınması.
- Belirlenen güvenlik politikası dâhilinde iç güvenlik organizasyonun şekillendirilmesi için bilgi sızıntısı saptama ve engellemenin başlatılması ve denetlenmesi.
- Bilgi sızıntısının engellenmesi için bilgi paylaşılan dış kurum ve kuruluşlarında belirlenen bilgi sızıntısı politikasına uymasının zorunlu kılınması.

- Bilgi, kurum ve kuruluşlar için değerli olduğu için, sızıntının azaltılması için bilginin sınıflandırılması ve bilgiye erişimde sorumluluklar verilmesi.
- Bilgi sızıntısının engellenmesinde, çalışan eğitimi ve yetkilendirilmesi denetiminin işe almadan önce, iş süresince ve işten ayrılış süreçlerinde devamlılığının sağlanması.
- İletişim ve operasyon yönetiminde, operasyonel yöntem ve sorumlulukların belirlenmesi, kötü amaçlı yazılımlara karşı koruma, ağ güvenlik yönetimi, yedekleme ve yedekleme ortamlarının güvenliği, diğer yapılarla bilgi değişimi ve bunların görüntülenmesi işleri bilgi sızıntısının saptanması, engellenmesi ve kayıt altına alınması ile ilgili önemli denetimleri sağlaması.
- Kullanıcıların ağ, uygulama ve bilgi erişimleri denetiminin bilgi sızıntısını azaltması
- Kullanılacak bilgi sızıntısı saptama uygulamasının sızıntı oluşması durumunda, raporlama ve yönetim yeteneklerinin iş gereksinimlerine uygun ve yardımcı olması
- İş devamlılığı için bilgi sızıntısı saptama uygulamasının da ölçeklenebilir olması

2.6. BT yönetiminde bilgi sızıntısı ile ilgili dikkat edilecek diğer konular

Günümüz bilgi sızıntısı dünyasında yönetimsel açıdan karar verirken göz önünde bulundurulması gereken birçok nokta bulunmaktadır.

Günümüz bilgi sızıntısı engelleme ürünleri genellikle veri üzerinde 2 tür işlem yapmaktadır.

1. Bütünleşik engelleme: Bilgi sızıntısı engelleme uygulaması ağ üzerindeki birçok protokolü takip ederek hassas verinin engellenmesini sağlar.
2. İndirgenmiş engelleme: Uygulama bilgi sızıntısını saptar ve saptadığı sızıntıyı engellemeyi gerçekleştirecek başka bir uygulamaya ya da vekil sunucusuna yönlendirir.

Yukarıda listelenen özelliklerden dolayı, bilgi sızıntısı uygulamalarına yatırım yapılacağı zaman, hali hazırda bulunan altyapıdaki özellikler ve bileşenler de göz önünde bulundurulmalıdır. Örnek olarak ağda, bazı protokoller üzerinde engelleme yeteneğine sahip bir uygulama bulunuyorsa bilgi sızıntısını saptamak ve bu uygulamaya yönlendirmek, daha verimli bir yöntem olabilir.

Bilgi sızıntısı terimi, taşınabilir depolama aygıtlarının güvenliğinden, e-posta güvenliğine kadar birçok çeşitli alanda sıkça kullanılır. Bu yüzden bilgi sızıntısı uygulamaları, bilgi sistemleri üzerinden bilginin sızabileceği bütün ortamlar ve kaynaklar düşünülerek tercih edilmelidir.

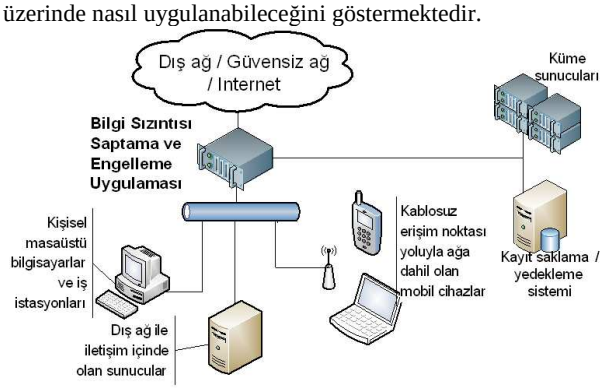
Bilgi sızıntısı ürünlerinin, piyasa üzerindeki çeşitliliği incelenecek olursa masaüstü/dizüstü bilgisayar yani uçbirim ve ağ tabanlı bilgi sızıntısı ürünlerinin kullanımda olduğu görülmektedir. Tablo 4'te bu ürünlerin kullanım oranları görülmektedir[10].

Tablo 4: Bilgi sızıntısı ürünleri kullanım oranları

	Uçbirim bilgi sızıntısı uygulamaları	Ağ tabanlı bilgi sızıntısı uygulamaları
Kullanımda	% 44	% 42
Önümüzdeki 12 ayda planlanan	% 16	% 14
İlgilenen	% 11	% 13
İlgilenmeyen	% 7	% 6
Bilgisi olmayan	% 22	% 26

3. Ağ Tabanlı Bilgi Sızıntısının Saptanması ve Engellenmesi

Bilgi sızıntısı olaylarının büyük bir kısmı ağ üzerinden gerçekleşmektedir. Daha önce belirtildiği üzere BT yönetimi için gerekli gizlilik, bütünlük ve devamlılık ölçütlerinin sağlanabilmesi için bir altyapı sağlanması gereklidir. Bu altyapı Tablo3'te görüldüğü üzere kurumsal ağın çıkış noktasına yerleştirilecek bir bilgi sızıntısı saptama ve engelleme uygulaması, bilgi gizliliğini ve bütünlüğünü koruyabilmeli ve işin ve uygulamanın devamlılığını garanti altına alabilmelidir. Şekil 1'de bu tarz bir uygulamanın, ağ üzerinde nasıl uygulanabileceğini göstermektedir.



Şekil 1: Bilgi sızıntısı saptama ve engelleme uygulamasının ağ içerisinde yerleştirilmesi örneği

Bunun için ideal ağ tabanlı bilgi sızıntısı uygulamasının sahip olması gereken genel özellikler şu başlıklar altında toplanabilir.

- Bilgi akışının düzenlenmesi
  - Saptanması
  - Kayıt altına alınması
  - Engellenmesi
- Güvenilir kayıt tutması
  - Hukuki delil oluşturması
  - Ölçüm ve değerlendirme yapmaya olanak sağlaması
- Performans
  - Ağ trafiğini belirli bir hız limitinin altına indirmeden gerekli taramaları yapabilmesi
- Ölçeklenebilirlik
  - Ağdaki veri akışının hacmine göre kullandığı altyapı kaynaklarını otomatik olarak düzenleyebilmesi
- Güncel protokollere destek vermesi
  - HTTP, SMTP, POP3, IMAP, FTP, MSNMS, Jabber, SFTP, SSH, Telnet, vb
  - Bu protokollerin SSL ile sarmalanmış sürümlerinin de denetim altına alınabilmesi

- Bu protokoller için ön tanımlı saptama yapabilmesi için geniş yelpazede şablon tanımlamalar sunması
- Özelleştirilebilirlik
  - Kurumların ön tanımlı protokoller dâhilinde kendilerine özel saptama yöntemleri oluşturabilmeleri
  - Kurumların ön tanımlı protokoller haricinde kendi kullanımlarına özel protokoller için saptama motorları oluşturabilmeleri

3.1. Ağ tabanlı bilgi sızıntısının saptanması

Bilgi sızıntısı uygulamaları için en büyük sorun, sızıntının saptanması konusunda meydana gelmektedir. Bu uygulamalar arasında farkın oluşmamasının en büyük sebebi sızıntı saptama motorları arasında belirli bir farkın ve dolayısıyla üstünlüğün bulunmamasından kaynaklanmaktadır.

Sızıntı saptama yöntemlerinden tam eşleme, sızıntı saptamada en çok kullanılan ve hatalı sonuç oranının en düşük olduğu yöntemdir. Birçok uygulama bunu ham bilginin girilmesi ya da dosyaların tek yönlü sindirim(hash) yöntemleriyle oluşturulan parmak izlerinden oluşturulan veritabanları üzerinden gerçekleştirirler. Ancak bu yöntemin başarılı olabilmesi için bu yöntemi kullanacak olan kuruluşun yapısal olarak geniş ölçekli tanımlanmış hassas verisinin olması gerekmektedir.

Diğer bir yöntem olarak, içerik analizi, düzenli ifadeler veya karmaşık sözlük analiz araçlarının kullanılmasıyla, bilginin değişik seviyelerde hassasiyetinin ölçülmesi için kullanılabilir. Bu yöntem, doğruluk olarak tam eşlemeden daha zayıf sonuçlar ortaya çıkarsa da, bilginin dağınık, tutarsız olarak tutulduğu veya kurum bilgisi üzerinde yapısal çalışmaların gerçekleştirilmediği durumlarda daha iyi bir performans ortaya çıkarmaktadır[11].

Üçüncü bir yöntem olarak, protokollerin kendileri için belirtilen amaçlar doğrultusunda kullanıldığından emin olmak için yapılan protokol kullanım denetimleridir. Bu denetim hiçbir uygulamada yer almamasına rağmen oldukça önemli bir saptama gereksinimidir. Örnek olarak HTTPS 443 numaralı bağlantı noktası üzerinden SSH tünellerinin açılması ya da DNS saldırıları sırasında anormalliklerin tespit edilmesi bu yöntem içerisinde gösterilebilir.

Diğer bir yöntem olarak, saptama sırasında, uygulamalar SSL ile sarmalanmış protokollerin incelenmesine olanak sunacak altyapıyı geliştirmeleri gerekmektedir. Bu yaklaşımın içerisine sızıntı saptama uygulamasına şifreli olarak gelen verinin dışarıya çıkmasının engellenmesi de eklenebilir.

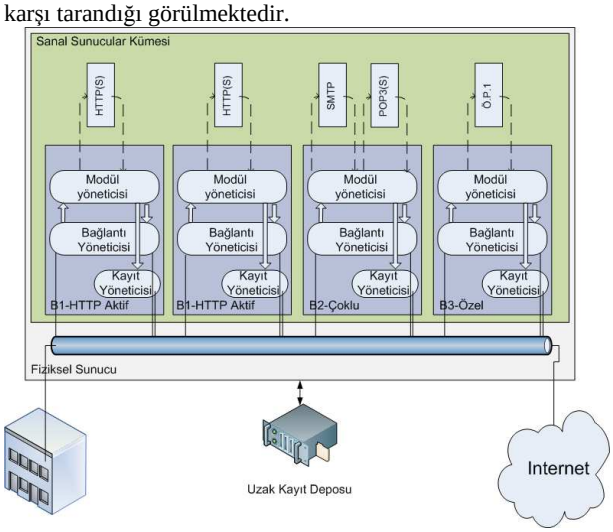
Özellikle Internet ve e-posta protokolleri üzerinde bilgi sızıntısının azaltılması ve saptanması ile ilgili çalışmalar son dönemde yoğunluk kazanmıştır[12][13].

Bilgi sızıntısı tespiti, klasik BT yönetimi uygulamalarını gerektirdiği için, saptanma için kullanılacak yöntemler için önce planlama yapılması ve hangi bilginin grubunun risk taşıdığının bilinmesi bu işlem için fayda sağlayacaktır.

3.2. Ağ tabanlı bilgi sızıntısının saptanmasında performans ve ölçeklenebilirlik

Ölçeklenebilirlik ve performans, bilgi sızıntısında hizmet devamlılığı açısından, yoğun ağ trafiğinin incelenmesinde önemli bir gereksinimi oluşturmaktadır. Genelde ikili kod metinlerinde örüntü eşleme yapmanın gerekeceği bir uygulama olarak bilgi sızıntısı saptama işleminin, eşzamanlı çalışma performansının yüksek olduğu ve örüntü eşleme işlemlerini kolaylaştıran Erlang[14] gibi fonksiyonel programlama dilleriyle gerçeklenmesi faydalı olacaktır[1].

Diğer bir ölçeklenebilirlik yöntemi olarak sanallaştırma, altyapı ve donanım kaynaklarının daha verimli kullanılmasını ve yönetim kolaylaştırılmasını sağlayacaktır. Üzerinde saptama işleminin gerçekleştirilmek isteneceği her protokol için bir veya birden fazla sanal makineyle işlem uygulanması, hata oranını azaltacaktır. Ağ trafiğinin yoğun olduğu zamanlarda yedek sanal makinelerin, aktif veya pasif hale getirilmesiyle bilgi sızıntısı saptama uygulamalarında ölçeklenebilirlik ve hizmet devamlılığı sağlanmasında bir ön koşul olarak aranmalıdır. Şekil 2'de bir sanal sunucu kümesi içerisinde 2 sanal makinenin aktif olarak HTTP trafiğini incelediği, üçüncü sanal makinede SMTP ve POP3 trafiğinin incelendiği ve dördüncü sanal makinede özel protokol trafiğinin sızıntıya karşı tarandığı görülmektedir.



Şekil 2: Sanal sunucu kümesinde bilgi sızıntısı saptama

4. Diğer Güvenlik Teknikleri ile Karşılaştırma

Örnek olarak kurumumuzdan bir çalışanımızın ya da içeriye sızmış bir bilgisayar korsanının, HTTPS protokolü üzerinden dışarıya bilgi sızdırmak istediğini düşünelim. Bu senaryo dâhilinde ateş duvarı(firewall), içerik filtreleme yazılımı ve saldırı tespit sistemi ile bilgi sızıntısı uygulamasının karşılaştırmasını gerçekleştirelim.

Eğer ateş duvarı(firewall) ile bu sızıntı engellenmek istenseydi, yapılabilecek tek işlem, HTTPS bağlantı noktasını yani 443 numaralı noktayı kapamak olacaktı. Ancak HTTPS, kurum içerisinde ve dışarısında ve özellikle Internet üzerinden birçok bilgiye erişim için gerekli olacağı için riski engellemek için bilgi erişimi kısıtlanmış, dolayısıyla genel iş verimliliği azaltılmış olacaktı.

Eğer içerik filtreleme(content filtering) yazılımıyla bu sızıntı saptanmak istenseydi, HTTPS bağlantısı SSL ile sarmalanmış olduğu için filtre işlem yapamayacaktı. İçerik filtresi bir şekilde SSL bağlantısında araya girmeyi başarsa bile, web içerik filtreleri yapısal olarak içeriden dışarıya çıkan veriyi

[1] Ekim 2009 tarihi itibariyle erişilebilir durumdadır. http://www.sics.se/~joe/apachevsyaws.html

değil dışarıdan içeriye gelen veriyi incelerler. Bu yüzden sızıntıyı tespit edebilmesi mümkün olmayacaktı.
Saldırı tespit sistemleri(Intrusion detection system) ise örüntü tanımlamaları üzerinden çalışmaktadırlar. Ancak HTTPS verisi şifreli olarak sistem üzerinden geçtiği için herhangi bir ön tanımlı örüntü ile uyuşması mümkün değildir.

5. Sonuç

Bilgi sızıntısının saptanması ve engellenmesi süreci BT yönetimi risk süreçlerinin bilginin sınıflandırılması ve hassas verinin dışarıya akışının engellenmesi anlamında önemli bir kısmını oluşturmaktadır. BT yönetimi açısından gerekli ölçütlerin karşılanabilmesi ve yatırım geri dönüşünün sağlanabilmesi için tesis edilecek bilgi sızıntısı saptama uygulamasının; bilgi akışını düzenleyebilmesi, güvenilir kayıt ile ölçüm ve değerlendirmelere dayanak oluşturabilmesi, iş gereksinimlerini karşılayabilecek performans ve ölçeklenebilirlik metriklerini karşılayabilmesi, ön tanımlı protokol ve saptama yöntemlerine sahip olması ve birçok açıdan özelleştirilebilir olması gereksinimleri göz önünde bulundurulmalıdır.

6. Teşekkür

Makale yazarları COBIT ve ISO/IEC 27002 çalışmalarında yer alan tüm araştırmacılara teşekkür eder.

7. Kaynakça

[1] COBIT 4.1 Framework, Control Objectives, Management Guidelines, Maturity Models, ITGI, 2007
[2] ISO/IEC FDIS 17799:2005(E), http://www.iso.org/iso/catalogue_detail?csnumber=50297
[3] Proofpoint, Outbound Email and Data Loss Prevention in Today's Enterprise, 2008
[4] Güvenilir Bilişim Grubu, http://www.trustedcomputinggroup.org/
[5] M. Rosenblum and T. Garfinkel, Virtual Machine Monitors: Current Technology and Future Trends. IEEE Internet Computing, Mayıs 2005, Sayı 38, Nu. 5.
[6] ISO International Standard ISO/IEC 15408-1:2005, Second Edition (October 2005)
[7] Information Systems Audit and Control Association (ISACA), http://www.isaca.org
[8] IT Governance Institute, http://www.itgi.org
[9] Sahibudin, S.; Sharifi, M.; Ayat, M., Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations ;Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference, 13-15 Mayıs 2008 Sayfa:749 – 753
[10] Oltsik J., McKnight J., Gahm J., Protecting Confidential Data Revisited, ESG, Nisan 2009
[11] DLP Experts, Data Loss Monster: Beware The Pitfalls of DLP Deployment, http://www.dlpexperts.com
[12] Borders K., Prakash A., Quantifying Information Leaks in Outbound Web Traffic, 2009, 30th IEEE Symposium on Security and Privacy
[13] Carvalho, V.R., Cohen, W.W.: Preventing information leaks in email. In: Proceedings of SIAM International Conference on Data Mining (SDM 2007), Minneapolis, MN (2007)
[14] Gustafsson P., Sagonas K., Applications, Implementation and Performance Evaluation of Bit Stream Programming in Erlang, Ninth International Symposium on Practical Aspects of Declarative Languages (PADL'07)